RBR Check Fraud.mp3

Speaker1: [00:00:09] It's time for a special episode of Regions Business Radio. Now, here's your host, J.D. Mealor.

Speaker2: [00:00:20] Thank you Mike Sammond and JD Mealor here with Regions Business Radio. So good to be back with you. And we have a couple of episodes. We're going to start with episode one of a series that we're introducing for 2024 on the importance of fraud awareness, fraud protection and how to protect yourself, your business, your clients, your vendors from, uh, this this dreaded word called fraud. You know, fraud continues to impact businesses, individuals, and families across our nation. We've seen we've seen a high volume of it, specifically in our footprint, which many of you know, is the footprint of the Southeastern Conference, the SEC. But we're going to talk over this series of episodes. We're going to talk about three different fraud events. And we are so blessed to have a very good friend of mine, Jeff Taylor, with us today. Jeff made the ride over to Metro Atlanta from Metro Birmingham. So Jeff, welcome, happy to have you here. Thank you JD, it's.

Speaker3: [00:01:28] An honor to be here. Thank you so much.

Speaker2: [00:01:30] Oh well, it's an honor for you to be with us as well. And as I mentioned, we're going to have we're going to have a few episodes our episode today. We're going to focus on check fraud. But before we do, tell us the Jeff Taylor story and how in the world did you get involved with bank fraud?

Speaker3: [00:01:55] Well, I've been in banking now, gosh, 26 years. I started out in our merchant services and acquiring credit card acquiring area, moved into our corporate banking group, managing our customer service area for another financial institution. Adding to that, our account analysis area and then even our implementations group and then moved from there into treasury management, doing more some special project work, but also attempting to help from the standpoint of helping customers understand some of the risks around payments and some of the things to do with payments, and then moved into a more payment related transaction activity position where I managed a group that did our payables, receivables and Fraud Solutions products and then moved from there into this area of fraud, representing the commercial bank and our

commercial clients in how they understand fraud, how they are educated about fraud, to continue to bring them up to speed on the different attack vectors that are out there and ways that they can remediate those and things that they can do for on their side of the payment transaction to help.

Speaker2: [00:03:13] And those topics are going to be what we're talking about over this series. This this three-part series, as I mentioned today, is going to be about check fraud. But before we get to that point, you have you've spent years in banking. You're talking about payables, receivables. All of those areas are ripe for this fraud battle that we're in. So your unique perspective, your unique ability, as some would say is, is from that view of, you know, how payments are processed and, and what we can do to protect those. And I would imagine in your previous life still keep them efficient, not only safe and all those things. So your perspective on it is meaningful not just to our current clients, but maybe we have listeners that aren't a current client of regions Bank, and this applies to them as well. Absolutely. Very good, very good. Now to our episode on check fraud. Checks have been around for a long time. That's the most basic way, I would imagine, other than cash and coin, for paying for product services rendered. You know, whatever the case may be. So can you provide some background on this check fraud sort of threat, if you will? I love when you say vector, by the way, um, can you talk about the check fraud threat and why it's important and what what's that all about?

Speaker3: [00:04:43] Well, absolutely, JD, I mean, in years past we had so much confidence in writing a check. We, we felt like that, that there were few, if any, risks associated with writing a check. But the fraudsters have picked up on that. And, and this goes back years and years to the ability of, of a fraudster to somehow intercept a check and capture the information that's there to alter information on that check and then attempt to deposit the check themselves or into an account that they control or in some other fashion, cash, the check, other things that. They're able to do with that instrument once they are able to obtain it. The Association for Financial Professionals administers a survey every year. And that survey indicated that 63% of companies who responded to the survey indicated that they had been a victim of check fraud. So 63%, I mean, six out of ten companies that responded, said I. I have been a victim of check fraud in some fashion.

Speaker2: [00:05:46] That is a big number. It is big. So we're in the north Atlanta region in Duluth, Georgia. And a friend came by. They're about to have their big chamber event in this venue a week from now. Well, J.D., why are you bringing that up? Because this room that we're in will be filled with thousands of business owners and executives. And you're telling me that we're in. They're in here. Six out of every ten of those companies that are represented have likely been a victim of check fraud, right? Yep.

Speaker3: [00:06:15] And I really think, J.D., those numbers are going to go even higher. Okay.

Speaker2: [00:06:19] This wasn't part of part of our outline, but when you say that, it makes me want to ask you a couple of questions. What information is on a check that a criminal or a fraudster wants to get a hold of? Yeah.

Speaker3: [00:06:34] So there are four critical elements if you think about it. The first is that a that paper instrument gives the fraudster the ability to see what the check stock looks like. Okay. What color do you use. Are you using a specific color consistently? Do you have a background? Is there something in that in the document itself that they need to know about? Okay. The second thing is that that they're able to see the check number or the range the check number range that might be involved. So if that that check number is 1020, then they have an idea that give or take ten checks before ten checks after are going to be in that same general range. The third thing that they are able to get is an example of the authorized signature. So even though we oftentimes our signature may be scribbled or it may be eligible, they still have a copy of that of what that authorized signature looks like. Yeah. And then the fourth thing, and probably the most critical, is that they're able to capture the routing and transit and account number that's at the bottom of that check. And that's what we use as a financial institution to process that item.

Speaker2: [00:07:48] Yeah. I spoke to a group of executives from our local school systems last week, and I brought up the fact that the routing and transit number is on there, and it's something that we need to protect. But I forget about the signature, and I never would have thought about the check number. Now, you mentioned what the check looks like. I'm not. You could go to a local office supply place and get a check stock, can you not?

Speaker3: [00:08:13] Exactly, exactly. You can buy a generic check stock. And it's pretty easy to create counterfeit checks using that information that that we just talked about. And that's one of the critical things around the range when you think about the check numbers. So if the fraudster is intent on creating counterfeit checks, they have a sense of what that range looks like so that they might be able to bypass some of the the technique that's used to identify a fraudulent item.

Speaker2: [00:08:42] Okay, okay. And again, just my own curiosities here. Can you explain how as best as you can. Because I'm really hoping that you've never actually done this before.

Speaker3: [00:08:54] I'm not a fraudster.

Speaker2: [00:08:56] When you hear of the tum washing a check or if they if they if someone physically gets a check, what can they do to it to deface it and then sort of write it to them. So how does that my mind can't even comprehend how that works.

Speaker3: [00:09:11] There are chemicals that are available that enable the ink to be erased, basically off of that check. And so when they when the fraudsters do that, they're able to they can remove any information that was written on that check in ink. So they can take the they can change the dollar amount. They can change the payee name. They can change the line underneath.

Speaker2: [00:09:36] That's like the memo line. Yeah.

Speaker3: [00:09:38] Well the memo line if that's important or the information that that explains the total dollar amount.

Speaker2: [00:09:44] Yeah okay. Yeah I know this this isn't why you're here. But are they taking that check and they're able to wash everything off of it. Or are they literally taking these chemicals and sort of erasing. You get what?

Speaker3: [00:09:58] Yeah, I think it's both I mean, in some cases amazing. Well, in some cases they will actually erase all of the ink information that's on a check. So in

essence what they've got to blank check blank one with the routing and transit and account number on it. And then it's typically what they're trying to do JD with the information. So. As an example, if the intent is to sell those checks on the dark web and monetize them that way, then they may wash all of that ink information off so that they're basically selling a blank check with a routing and transit and account number on it.

Speaker2: [00:10:35] There's a market for that.

Speaker3: [00:10:36] Oh, absolutely. On the dark web. Sure.

Speaker2: [00:10:39] Where's the dark.

Speaker3: [00:10:39] Web? Well, that's a long explanation. Okay.

Speaker2: [00:10:42] We won't go there. I'll save you from that.

Speaker3: [00:10:44] I'll try to simplify it. When you think about the internet, what we know of and what we use on a regular basis on the internet is the is the top of the mountain, the examples of the top of the mountain and then the or like a glacier, the top of the glacier, the water line. And then what's all underneath it? Yeah. What's underneath the water line is the dark web really? And we, you and I, we could have access to that information if we chose to use it. But the criminal element uses that information through specific browsers and specific protocols that enable them to get to the criminal enterprise that is, that is publicized on the dark web.

Speaker2: [00:11:27] Okay, my mind is being blown. I've gone from, you know, routing number, transit number. Now we're talking about check ranges. We're talking about dark web. And this is important for you as a listener to Region's business radio today, because you may find it entertaining. Jeff's knowledge is certainly beyond impressive, but this could happen to you if you're not careful. We're going to talk about that in a minute. One of the questions we wanted to talk about is, would you say that writing checks is still sort of popular in business today? Have you seen maybe check volumes decreasing over time? How popular is check usage in today's business environment.

Speaker3: [00:12:05] Yeah. And I want to back up if I can. Just a second JD okay. It's not just the dark web. So this information is being publicized in other channels. Some of them are publicly available. And so it's a broad spectrum of usage where the fraudsters are basically promoting the capability to do this. And it's really scary. So when you talk about the volume of checks, you know, if you think from a consumer standpoint we write fewer and fewer checks. Yeah. And this may be may seem odd coming from a banker, but as consumers write fewer and fewer and we provide most financial institutions provide a pretty robust online banking capability that enables an individual to use bill payment software and enter their information and the bills that they're going to be paying into that software to create more digital payments. But still, some of those payments end up being a check, depending on how on the capabilities and the way that the receiving institution accepts those payments. Gotcha. So when you see from a consumer standpoint, the number of checks are declining, I think from a commercial standpoint, we're seeing a decline in checks, but it's not it's decreasing at a at a slower rate. Is that right. So okay, while we see more and more companies are moving to digital alternatives, you know, things that we're providing to them. Ach same day ACH real time payments and the what will become the introduction of a of another real time payment rail fed now. So there are a number of different other alternatives that commercial clients can use. But there's still a lot of controls on their side of the payment transaction that need to be put in place, even when they're moving to those digital alternatives.

Speaker2: [00:13:59] Gotcha. Gotcha. Checks remain easy to write and easy to steal.

Speaker3: [00:14:03] Exactly. I mean, it's still I think that's the main reason why we continue to see checks being a part of the, the, the payment protocol is that they're just it's just easy. It's what we've always done. Why should we change? It's just a matter of time though, before one of those checks is either stolen out of the mail or intercepted in some fashion to and creates a creates an issue.

Speaker2: [00:14:28] Great point. You know, I jumped ahead a minute ago asking what the fraudsters do once they get the check. Yeah, I failed to ask how.

Speaker3: [00:14:35] Do they get it.

Speaker2: [00:14:36] Right. Yeah. That's right.

Speaker3: [00:14:37] How do they. So it's really become easier and easier. The US Postal Service has reported thousands of assaults on postal workers, and tens of thousands of actual reports of intercepted mail and stolen mail. It comes a number of different ways. Oftentimes, what has happened is that the fraudster will literally hold up the Postal service worker while he's on his route and will steal the trays of mail out of the back of the truck. They take those to a house somewhere local, and they'll sort through those trays of mail to get all the things that they that they could use to monetize.

Speaker2: [00:15:18] Statements.

Speaker3: [00:15:20] Bank statements. Bank statements. Anything. If you think about it, what? What information is in those trays of mail that would enable me to create a synthetic identity, to impersonate someone, all of that information, they're able to monetize that information in some way. And then, of course, stealing the checks out of the mail when they pulled those, they're able to then go through that process of of washing them. Some of them may just be sold the way they are, and enable someone else to wash those checks and take the ink information off of there.

Speaker2: [00:15:54] Can you track them down? Can you track stolen checks down?

Speaker3: [00:15:57] Not really. I mean, you think about I mean, obviously if they're delivered in in something other than just regular mail, then there is the possibility of having a tracking number or some information that would help you track them. But but even still, you're tracking a package. You're not tracking the check itself. That's right. So you're not tracking what's inside of the package. So if that package is intercepted, then what's inside of it goes a different route. Yeah, it may go a different route.

Speaker2: [00:16:26] We have a we have a client locally that that had a high volume of checks written. And they've been impacted by check fraud. And, and we literally just had a cup of coffee and brainstormed how in the world do we get past this. And we they've attempted to reduce their US Postal Service mailing and move it to, you know, more of a commercial FedEx, DHL, UPS type of thing where there is a tracking number and they

know that. To your point though, whatever is in that package makes it to its destination, because in this case it was things just weren't getting where they were supposed to go.

Speaker3: [00:17:05] Yeah, absolutely. And I think to not putting those checks in your mailbox and leaving them in your mailbox, and this applies to consumers also, you know, you think about what we do when we put a letter in the mailbox in front of our home is we pull that red flag. Well, that's a yeah, that tells a fraudster there's mail in that box. And so if you think about it, they're cruising a neighborhood. They look at the mailboxes that have mail in them. So one of the suggestions we always try to make is, is to if when you can avoid using a window envelope because those are typically used for for mailing a check. Yeah. The second thing is don't put the check in your mailbox, but actually deliver the check to the US Postal Service office and hand it to that postal worker over the counter. That doesn't stop it from being intercepted once it goes into the mail system, but at least you know that it's not going to to be taken out of one of the blue boxes or out of a mailbox somewhere.

Speaker2: [00:18:07] Now, if you're listening, and it may sound like we're picking on the US Postal Service, it's just.

Speaker3: [00:18:12] Not it's just the.

Speaker2: [00:18:12] Delivery primary delivery method. Outside of that, where do we see check fraud occur? Does it occur elsewhere outside of the US Postal Service?

Speaker3: [00:18:22] Sure. I mean, just like we talked about. I mean, it's not difficult when you intercept that package. What's inside of that package can go any kind of different route. So it's certainly not unheard of for that to happen. And there are ways where if you have an inside situation, as an example, you could have a rogue employee who is responsible for depositing all those checks, all that information is available to them, and to be able to take a photograph of that check to create something counterfeit. Long term. I mean, there's all kinds of other different opportunities where those checks can be acquired.

Speaker2: [00:19:01] I love this format for the conversation, because every time my mind is racing, because what you know and what you've experienced, it's I can't

imagine that somewhere this morning, a person got up to go to work, and their job was to wash a check and create a fraudulent. Yeah, I.

Speaker3: [00:19:20] Mean, it's an industry. It literally is. I think of.

Speaker2: [00:19:22] Industry as a.

Speaker3: [00:19:23] Criminal enterprise, but it's an industry.

Speaker2: [00:19:25] I just I mean, it's not, you know, tourism or, you know, manufacturing. We don't we don't look up a next code on or an SIC code on, you know, criminal enterprise. But it's sad that we have to deal with that. And as much as I want to have this conversation be somewhat lighthearted, but still very, very specific, if you're listening today, you've got to pay attention to what Jeff Taylor is telling you, because you may think, well, it hasn't affected me, I would add yet. Exactly. It's going to six out of ten. And how many times do you, as a business owner as or an executive, have the opportunity to listen to someone with Jeff's experience? Tell you, I don't think you're a fortune teller, but your experience tends to indicate that. This is likely to happen to 6 or 7 eight out of every ten people listening to this. That's right.

Speaker3: [00:20:23] Yeah, definitely not a prophet, but I can pretty much assure you that somewhere along the line, that client who writes checks consistently is going to have is going to be impacted in some way.

Speaker2: [00:20:32] Without a doubt.

Speaker3: [00:20:33] Right. And, you know, J.D., a lot of times these situations are not discovered for months. So if you think about what the typical payment cycle is, a vendor may not reach back out to you and tell you that they did not receive your payment for 60 or 90 days. And so by that time, there's so many other things that have occurred that would enable or keep anyone from being able to track that item or recover that item in any way.

Speaker2: [00:21:03] And as much as there's sometimes legal time frames within, you know, credit opening or, excuse me, deposit opening agreements whereby you have to

notify the bank of fraud of any fraudulent events. What we've seen is, to your point, sometimes vendors don't do a good job of running their accounts receivable. And it may be 90 days later and they're calling you up and saying, hey, Jeff, you owed me, you know, some money a couple months back. Where is it? Well, I sent it, and the money is literally gone.

Speaker3: [00:21:36] By that time, the fraudsters have typically moved that money out of the first drop account that they're using and moved it into others, breaking the transaction into smaller transactions, making them more difficult to track. And they're astute about that. I mean, they know what they're doing and they are very capable.

Speaker2: [00:21:53] As much as I'm thinking about business owners and executives that may be listening, you know what you do very well. You may manufacture something. You may have a service business. Maybe it's a cleaning business. Whatever the case may be, I'm looking at Mike salmon, who does a wonderful job of producing podcasts and doing promos. Yeah, he's very good at what he does. The criminals are equally good at what they do. You get good at what you practice, right? So they're really good at it. And I'm saying it that directly because while you Mr. and Mrs. Business owner while you Mr. and miss business executive while you're doing what you do so well the criminals are doing that also and we want to raise the red flag, as we say at regions to pay attention to this. So if it sounds like we've gotten to the point of this podcast where we're trying to scare you, it's because we are now, Jeff, what happens after fraud?

Speaker3: [00:22:48] Yeah, I'm pretty good at the scare you part. The yes you are. The remediation part is much more difficult, you know, so there are some things that are industry suggested practices that that we suggest that clients put in place. The first one is reconcile your account regularly. You as an individual business owner need to be looking at that account activity every day, typically through your commercial online banking platform you've got access to either previous day activity, current day activity. So you can see the transactions that are that are posting to your account. If you see anything unusual whatsoever, you need to contact your financial institution immediately, even quicker.

Speaker2: [00:23:30] Yeah that's right. If there's anything quicker than immediate, it's got to be that quick.

Speaker3: [00:23:33] The second thing is, anytime you realize that check stock is missing, you want to make sure that you put a stop payment on that check, or you put stop payments on a range of checks. If you realize.

Speaker2: [00:23:46] Can I play devil's advocate on that point? Well, if I put a stop payment, it's $15 a check and you're the bank, you should protect me from fraud. I'm role playing here. I'm, you know. Well, I don't want to. I don't want to put stop payment because it'll it'll cost me something. It'll, you know, whatever the amount is. And, Jeff, you're my bank. You should be protecting me from this anyway.

Speaker3: [00:24:09] Well, I mean, I think the thing you have to do, J.D., is look at what's my average vendor payment. Okay. What's my average vendor payment? Let's say it's $2,500. Yeah. How many items can you pay for in that $2,500? How many stop payments could you pay for in that $2,500 that would keep it's like it's almost like an insurance policy. Yeah. You pay for those things to ensure that that transaction is not going to be that you're not becoming a victim in that case, that that transaction is not going to be processed.

Speaker2: [00:24:43] Yeah.

Speaker3: [00:24:43] Or those counterfeit checks are not going to be created. Yeah.

Speaker2: [00:24:46] I think that I'm going to speak for Jeff and I together, because we've been through this a lot over the last 12 to 14 months. Jeff and I specifically have worked on millions of dollars of fraud impact. I guess impact would be the right time. And in those situations, a simple investment in technology or maybe a stop payment could have prohibited substantial losses. Right. And I think what's sad is your mind goes automatically to we may be out 2030. Grand, $2 million, whatever it is. What you fail to think about is the impact it has on a business, on their employees, on people at home and the criminals. They're not thinking about Jeff Taylor. And you know what? They want the money and they want to. It's a small investment. I'm begging you to recognize it. Yeah. If you if you find that check stock is stolen, you got to you got to put a stop

payment on everything that you know is missing and monitor that. I was I was I was telling Jeff earlier that I had an experience where a client confessed to me that they had signed checks in a drawer, and when somebody needed them, they would just go by and get them. They moved offices and then that check stock was missing and they didn't panic about it. That's what that's what blew my mind. How are you not panicking, running to the bank practically to stop it? We're doing the best we can with the information that we have to help protect you. Sometimes, you know, we need more information from you in the form of a product called positive pay, which is what I always think about with check fraud.

Speaker3: [00:26:28] Absolutely. You know, and I mentioned the example I used, it was $2,500. Think about the multiplier effect. If that average vendor payment is 25,000 or 250,000. Yeah. You know, it's a business decision that you have to make obviously. But it's one that is foundational. So you've got to be able to to think about that and make those kinds of plans as far as your business is concerned. The third thing that we would suggest, obviously, is to convert those checks to an electronic alternative, some digital alternative ACH same day ACH real time payments, something that is more digital. But keep in mind you still have to make sure that you put the right controls in place on your side of that payment to help protect yourself. Things like dual control things like multi-factor authentication, least privileged access as an example, to be able to only provide an individual access to formats and platforms that they need in order to do their job.

Speaker2: [00:27:31] And I think all sophisticated online banking products, I'm not not the we call it our treasury. It is a fully implemented platform. It is not your online business banking thing that you would access, you know, through the public website. It is multi-channel authentication. But when you get into a more sophisticated online banking platform you can limit access to certain things. You can give users very specific purposes. They can get in and do that one thing. And you know don't be afraid of of hurting someone's feelings in your organization. If you want them to do one specific thing, give them that access because the information is it's so broad in a company, it's critical.

Speaker3: [00:28:17] So and you can also set up different alerts for different transactions and different changes that that will alert the administrator of the program to your program, to what? To what has occurred in that case. Yeah. The fourth thing we

always talk about is securing, as you mentioned in your example, securing your bank statements, securing your check stock, all those things. And then fifth, you also mentioned positive pay. It's just critical. If you are going to continue to write checks, you got to make sure that you have positive pay with payee name verification. Amen. As a part of your protection mechanism for check writing.

Speaker2: [00:28:57] Yes, for every check write. And again, I hate to go back to that and I apologize for bringing it up again. It sounds like I'm repeating myself, but there's a fee. Banks. Banks will typically charge an implementation fee or a monitoring fee for positive pay with payee name verification and give us positive pay one on one very, very simple intro for someone that may not be familiar with it.

Speaker3: [00:29:21] Sure, there are a number of different variations of positive pay. One of the most simple is one that that we call reverse positive pay. And that's where every check that you write is considered an exception and requires a decision. So you would receive from us on a daily basis information of the checks that are going to post to your account or that that have posted to your account, and then you have the option to return any of those checks that you deem to be either counterfeit or altered in some way. Where that information is, is not what you intended it to be.

Speaker2: [00:29:58] Do they get an image? Is there an image from which to make a decision?

Speaker3: [00:30:02] I think they can. They can actually see that image and and see the item itself.

Speaker2: [00:30:05] Okay. And that's a reverse positive pay. We, we sort of we sort of put a stoplight on everything that comes through. Right. And we want the client to review them and verify that their, their actual. Instruments that should be honored and paid. That's right. Okay.

Speaker3: [00:30:20] The other more sophisticated version is called next day or same day positive pay okay. That typically requires that the client provide us with what's called an issue file. So they send us a file out of their enterprise resource planning program, that platform, their check writing platform and their accounting software. And they tell

us, here are the checks that we have written and the items that we have written that we expect to be posting to our account. And then every day we systematically compare that issue file with the items that are posting to their account and then provide them with those exceptions.

Speaker2: [00:31:01] Okay. Now does that system feed into our teller system?

Speaker3: [00:31:07] It does.

Speaker2: [00:31:07] So. So if if there's a fraudulent if you see an exception, then our tellers would be aware also that that there's a flag that this might be a fraudulent check or whatever. Yeah.

Speaker3: [00:31:18] In the more sophisticated versions the teller system is is integrated into that process. So yes, they would see that if.

Speaker2: [00:31:26] You think about check fraud and, you know, we're talking to business owners and, and executives that they're running maybe a $200,000 business all the way up to a 203, $400 million business in revenue. That's just how my mind works. So forgive me for asking a question that may sound a little clunky, but how much time? How much time should an executive team focus on this? I know it's a broad question, but in my mind I'm thinking about maybe they have a weekly executive meeting and they're planning the week ahead. This just seems like a topic that an executive team of any company or an owner or an executive, even if it's a family-owned business and they're around a dinner table, you need to be talking about this.

Speaker3: [00:32:12] There are industry suggested practices around all of that, and one of them is just it's a risk-based decision. So you as a business owner, you have a plan about how you're going to distribute your product market, your product, what your annual plan may be for growth, for acquisition, for hiring new employees. Just like that, you've got to think about what your continuity plan is going to be when you become a victim of fraud. So it's just like your business continuity plan. If your business were interrupted by a natural disaster, you've got a plan as to how you're going to recover. It's the same situation with fraud. So you've got to be able to understand and make a

decision about what's my risk tolerance in this. Yes. And decide as a, as a, an executive committee what that risk tolerance looks like.

Speaker2: [00:33:07] You answered the question better than I asked it. So thank you for doing that. And I, I want to just it's subtle. But Jeff said when you're a victim of fraud not if because it's it is it is that rampant. We talked a lot about fraud. We talked specifically about check fraud. Any closing comments, any warnings, anything in closing regarding check fraud that you would like people to know or take action on?

Speaker3: [00:33:33] Well, I think you mentioned it, JD. I mean, I think it's important to know this this attack vector continues to grow and it's not going away anytime soon. I think that as part of that risk tolerance and understanding that risk posture, it's creating this cyber and fraud awareness mindset. All the things that we talked about today, none of those, even all of them, in conclusion, are not going to 100% prevent you from being a victim. That's right. They can't do that. You know, there's nothing that's going to do that. But what it will do is it helps you to create that education and awareness. It helps you to protect yourself. It helps you to take advantage of the opportunities that are available to you to protect yourself. So I think it's important that businesses, to your point that businesses recognize that the risks are out there and begin to help themselves prepare for those risks.

Speaker2: [00:34:31] We talked about executive team, do you have a feel for which executive CFO, COO, HR, or do you have a feel for who in someone's company should take the lead on this?

Speaker3: [00:34:42] You know, I think a fraud awareness mindset starts at the top. I mean, it's the CEO, it's the president, it's the board of directors. As a matter of fact, I mean, in some companies, publicly traded companies, the board has to dictate those kind of things and say, what are you guys doing to protect your systems, to protect the things that you are vulnerable, the areas where you're vulnerable, and make sure that you are protecting the company and the interests of the company.

Speaker2: [00:35:12] And then one final question, typically in a payment structure, when you're sending a check, a lot of times. Arms. I hear businesses say, well, I got to send a check because XYZ company only wants me to pay in check. I want to

challenge business owners and executives to change. Change the responsibility therein to the point that if if you have a vendor that only wants to be paid in checks, maybe you either tell them that you're going to send them an ACH or a wire, or there's other vendors that do what you do. I'm going to find one that because and I'm not saying violate a long-term relationship, I'm saying that that is both parties responsibility to protect one another from fraud. Right now, I'm getting passionate about it because I'm thinking about people that I know that own businesses and the people that work for them. Business owners never. Well, I like the saying a business owner doesn't go to bed worried about their mortgage. They're going to bed worrying about all their employees mortgages. The same thing applies in protecting everybody from fraud. If you have a vendor that refuses to take electronic payments and they only prefer checks, number one, honor the relationship and have a conversation about why they are in danger as you are. And wouldn't they want to help protect both of you from danger and then figure out how they how they can receive electronic payments?

Speaker3: [00:36:33] And I share your passion. It's a conversation that you just have with your vendor, and it's a part of having this robust vendor management program and being able to sit down with the vendor and explain to the vendor, look, here are the risks. Every time I send you a payment, I'm concerned about that. And I know you want to be paid on time. I know you want to receive your money on time because you need it. Let's move to a different alternative.

Speaker2: [00:36:58] Let's even get it there more quickly and more secure. Because I don't want to. I don't want to call you up 60 days from now and go, hey, we're missing this check. What are we going to do about it? Then? You're both out because the check writer has lost the money. The vendor who is expecting to receive the check has lost the money. Who has the money? The fraudsters, the criminals. And now you've rendered services. You've rendered a product that basically not going to be paid for to some extent, because then it gets it gets testy because legal gets involved and attorneys get involved. So again, in closing, business check fraud, if we can help you, if we can help you talk about this, we will put our team together. I've had Jeff on phone calls with clients before. Now his time is, you know, spoken for pretty broadly, but we can build a team around you to talk about this. And let me say that, hey, it's called Regions Business Radio for a reason. If you do not have a commercial or business banker that is

proactively talking to you about how to protect yourself from fraud, you need to call regions Bank.

Speaker2: [00:38:04] We talk about this on every one of our calls, even when I'm in the community, Jeff, even if it's not a, you know, a sales call or a service call, I'm always sounding the alarm in regards to fraud. So I would want you to know, at regions we make this a point to always discuss it. It may be the 10th time, it may be the hundredth time, or it may be the first time. But we're going to talk to you about fraud. Jeff Taylor, you are so good at what you do. You help so many people. Oftentimes you get called in after an event has occurred. And that's unfortunate. That's why today is important. Our first episode of this, this fraud series, is to let Jeff be the prophet that he is and tell you that if you don't take action now, you may face fraud in the future. Jeff, thank you for joining us today on Regions Business Radio.

Speaker3: [00:38:58] Thank you so much.

Speaker1: [00:39:04] Regions Bank, member FDIC equal housing lender. This information is general in nature and is not intended to be accounting, legal, tax, investment or financial advice. Regions believes this information to be accurate when recorded, but it cannot ensure that it will remain up to date, consultant, appropriate professional concerning your specific situation. The information should not be construed as a recommendation of a specific course of action for any individual or business. All regions, products and services are subject to qualification requirements, terms, conditions, fees and credit approval. Regions reminds its customers that they should be vigilant about fraud and security, and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices. As the threat evolves daily, there is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit regions.com backslash stop fraud or speak with your banker for further information on how you can prevent fraud.